How Spying and Surveillance Transformed Warfare from Analog to Digital and inadvertently created Cybercrime

From the smoky battlefields of World War II to the covert operations of the Cold War, the art of espionage and surveillance has undergone a metamorphosis, transmuting into the stealthy realm of cyberwarfare. This evolution has shattered borders, erased geographical limitations and attribution barriers, leaving no individual untouched. A journey through time unveils the profound implications of this transition, where poorly educated and managed Internet Assets have paved the way for an alarming surge in cybercrime, poised to become the world's top revenue generator.

During the Second World War, analogue spying reached its zenith. Intelligence agencies engaged in traditional cloak-and-dagger operations, using human assets and code-breaking techniques to gather classified information. These methods proved invaluable but were limited by geographical boundaries and risks of exposure.

The Cold War marked a paradigm shift as technological advancements birthed a new era of electronic surveillance. Espionage became a game of satellites, wiretaps, and hidden microphones, enabling global reach and deeper infiltration into rival territories. However, attribution remained possible, and the impact was contained to specific geopolitical spheres.

Fast forward to the digital age, where cyberwar has obliterated barriers. Nation-states and rogue actors now wage covert battles in cyberspace, targeting critical infrastructure, governments, and corporations often with near untraceable precision. The advent of poorly controlled and managed Internet Assets, Domains, Servers, and DNS unquestionably facilitates the ever-increasing rise of cybercrime, which has seen a threefold increase since 2020 making it equivalent to the world's third largest GDP behind China and the U.S. If cyberwar spoils and ill-gotten gains were added to the existing countries' GDP, the U.S. may be knocked off her No.1 perch.

Cybercriminals exploit exposed and insecure vulnerabilities in interconnected systems, perpetrating data breaches, ransomware attacks, and identity theft on a global scale. Without urgent attention to Internet Asset security, which includes Domains, Servers, and DNS, cybercrime is poised to surpass every other industry, becoming the world's No.1 GDP by revenue.

In conclusion, the trajectory of spying and surveillance has traversed from analogue to digital and cyber, blurring boundaries and altering the landscape of warfare. As the digital battlefield intensifies, the implications reverberate far beyond military and governmental realms, impacting every human being. To safeguard our interconnected world, a concerted effort to educate, control, and manage Internet Assets must be a top priority, curbing the rise of cybercrime and securing a safer future for all.

A J. Jenkinson

Andrew.jenkinson@cybersecip.com

27 July 2023